PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-195269
(43)Date of publication of application : 21.07.1999

(51)Int.Cl. G11B 20/10
G09C 1/00
G09C 1/00
H04L 9/16
// G06F 17/60

(21)Application number : 09-369395
(22)Date of filing : 26.12.1997

(71)Applicant : VICTOR CO OF JAPAN LTD
(72)Inventor : HIRATA ATSUMI
MACHIDA TOYOTAKA
HIROTA AKIRA

(54) INFORMATION CIPHERING METHODINFORMATION DECIPHERING METHODINFORMATION CIPHERING DEVICEINFORMATION DECIPHERING DEVICE AND INFORMATION RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information ciphering method by which a ciphering and a deciphering are relatively simply and inexpensively enabled and the estimation of a deciphering key is made difficult.
SOLUTION: An information control means 1 accumulates information key codes peculiar to digital information and information signals. A customer control means 5 accumulates customer peculiar certifying keys and reproducing device peculiar distribution keys. Thena code conversion means 9a converts the information key codes and generates work key codes. An information ciphering means 11a generates ciphering key codes from the work key codes and the sector numbers outputted from the means 9a. Thenthe sectored digital information data are ciphered by using the ciphered key codes.

CLAIMS

[Claim(s)]
[Claim 1]In an information encryption method which enciphers said digital

information data when recording on an information recording medium with a sector number which divides digital information data into two or more sectorsand shows rank of a sectorAn information encryption method enciphering said digital information data which carried out code conversion of the information key code peculiar to said digital informationgenerated a work key codegenerated an enciphering key code from this work key code and said sector numberand was sector-ized using this enciphering key code.
[Claim 2]In an information decoding method which decodes said digital information data of a recording medium with which digital information data divided and enciphered by two or more sectors is recorded with a sector number which shows rank of a sectorAn information key code peculiar to said enciphered digital information which is supplied from other than said recording medium is decodedCarry out code conversion of this information key codegenerate a work key codeand a decryption key code is generated from said sector number currently recorded on this work key code and said recording mediumAn information decoding method decoding enciphered digital information which is acquired by reproducing said recording medium using this decryption key code.
[Claim 3]Said work key code is divided into two or more partial bit string of the numbers of bits [information key code]After carrying out exclusive logical addition of the one arbitrary partial bit string chosen from this partial bit string to each of other partial bit stringrespectivelycombine it and the first bit string is generatedCarry out exclusive logical addition of the second bit string of the same number of bits as said information key code to said first bit stringand the third bit string is generatedAfter dividing into two or more partial bit strings of the numbers of bits [bit string / said / third] and rotating only the predetermined number of bits on the right or the left within each of this partial bit stringThe information encryption method according to claim 1 which generating the fourth bit string unitedlydividing said fourth bit string into two or more partial bit stringschanging array order of each partial bit stringand generatingor the information decoding method according to claim 2.
[Claim 4]The information encryption method according to claim 1wherein said enciphering key code or said decryption key code is the false random code sequence generated using a value just because it did division of said work key code with said sector numberor the information decoding method according to claim 2.
[Claim 5]In a data encryption device which enciphers said digital information data when recording on an information recording medium with a sector number which divides digital information data into two or more sectorsand shows rank of a sectorA code conversion means which carries out code conversion of the

information key code peculiar to said digital informationand carries out raw [of the work key code]A data encryption device having an information encoding means which enciphers said digital information data which generated an enciphering key code from a work key code outputted from this code conversion meansand said sector numberand was sector-ized using this enciphering key code.
[Claim 6]An information decoding device which decodes said digital information data of a recording medium characterized by comprising the following with which digital information data divided and enciphered by two or more sectors is recorded with a sector number which shows rank of a sector.
A key decoding means which decodes an information key code peculiar to said enciphered digital information which is supplied from other than said recording medium.
A code conversion means which carries out code conversion of the information key code decoded in this key decoding meansand generates a work key code.
An information decoding means which decodes enciphered digital information which is acquired by generating a decryption key code from a work key code generated in this code conversion meansand said sector number currently recorded on said recording mediumand reproducing said recording medium using this decryption key code.

[Claim 7]Said code conversion means is divided into two or more partial bit string of the numbers of bits [information key code]The bit string division / adding means which combines it and generates the first bit string after carrying out exclusive logical addition of the one arbitrary partial bit string chosen from this partial bit string to each of other partial bit stringrespectivelyAn adding means which carries out exclusive logical addition of the second bit string of the same number of bits as said information key code to said first bit stringand generates the third bit stringA bit rotation means which generates the fourth bit string unitedly after dividing into two or more partial bit strings of the numbers of bits [bit string / said / third] and rotating only the predetermined number of bits on the right or the left within each of this partial bit stringdividing said fourth bit string into two or more partial bit stringsand changing array order of each partial bit string -- work key code **** -- the data encryption device according to claim 5 characterized by thingsor the information decoding device according to claim 6.
[Claim 8]The data encryption device according to claim 5wherein said enciphering key code or said decryption key code is the false random code sequence generated using a value just because it did division of said work key code with said sector numberor the information decoding device according to

claim 6.
[Claim 9]Digital information data divided into two or more sectors is the information recording medium currently recorded with a sector number which shows rank of a sectorand said digital information dataAn information recording medium enciphering using an enciphering key code generated from a work key code which carried out code conversion of the information key code peculiar to said digital informationand said sector number.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to encryption/decoding method of informationand informationincluding a video signalan audio signala data signaletc.is sector-ized especiallyIt useswhen performing record/playback to information recording mediasuch as a diskand it is related with a suitable information encryption methodan information decoding methoda data encryption devicean information decoding deviceand an information recording medium.
[0002]
[Description of the Prior Art]The decode key (or information corresponding to a decode key) for decoding the enciphered information is recorded on the same recording medium at the same time it enciphers information using a predetermined enciphering key and records on a predetermined recording mediumwhen enciphering and recording information on a predetermined recording medium conventionally. In this casethe decode key (or information corresponding to a decode key) is distributed and recorded on record or two or more not continuous fields succeeding the continuous predetermined field of a recording medium.
[0003]Decoding had decoded the enciphered information which is reproduced from the same recording medium using the decode key obtained from the recording medium by reproducingor the decode key generated based on the information corresponding to a decode key.
[0004]Encryption is enciphered using one encryption key about at least one information. For examplewhen the information on the movie of the merit during 60 minutes was encipheredthe whole volume was covered for 60 minutes and it had enciphered using the same encryption key.
[0005]
[Problem(s) to be Solved by the Invention]The decode key (or information corresponding to a decode key) used in order to decode the enciphered information and its enciphered information conventionallySince it is recorded

on the same recording mediumand the one whole information was covered and it had enciphered using the same encryption keySUBJECT that it was easy to presume a decode key occurred. Since the decode key (or information corresponding to a decode key) was recorded in the information recording mediumthe field for it needed to be secured in the information recording mediumand the part and the fields which record original information were decreasing in number.

[0006]Comparatively easy and effective encryption/decoding methods include PN addition method by a common key system. This method is also called a pseudo-random addition methodand enciphers information using an M sequence coder. Howeverby trying decoding of the information which prepared two or more decode keys with fixed regularity for the contentsand was enciphered also by this method using them every oneand analyzing correlation with each decoding result and the regularity between decode keysIt is comparatively easily possible to presume the encryption key used for the enciphered information and its decode key. Thereforethere was a danger of decoding the enciphered information unjustly.

[0007]Although a block cipher systema public key systemetc. are variously proposed as a method of solving these problemsfor exampleSince all were complicated and required time for decoding processingthere was a problem that it was unsuitable or an expensive device was needed etc. in encryption processing of the information which needs to be played in real timesuch as a movie and music.

[0008]Thenthis invention is comparatively easyencryption and decoding are cheaply possible for itand an object of this invention is for presumption of a decode key to provide a difficult information encryption methodan information decoding methoda data encryption devicean information decoding deviceand an information recording medium moreover.

[0009]

[Means for Solving the Problem]As a means for attaining the above-mentioned purposethe following information encryption methodinformation decoding methodsdata encryption devicesinformation decoding devicesand information recording media are provided.

[0010]1. In information encryption method which enciphers said digital information data when recording on information recording medium with sector number which divides digital information data into two or more sectorsand shows rank of sectorAn information encryption method enciphering said digital information data which carried out code conversion of the information key code peculiar to said digital informationgenerated a work key codegenerated an enciphering key code from this work key code and said sector numberand was sector-ized using this enciphering key code.

[0011]2. In information decoding method which decodes said digital information data of recording medium with which digital information data divided and enciphered by two or more sectors is recorded with sector number which shows rank of sectorAn information key code peculiar to said enciphered digital information which is supplied from other than said recording medium is decodedCarry out code conversion of this information key codegenerate a work key codeand a decryption key code is generated from said sector number currently recorded on this work key code and said recording mediumAn information decoding method decoding enciphered digital information which is acquired by reproducing said recording medium using this decryption key code.
[0012]3. Said work key code is divided into two or more partial bit string of the numbers of bits [information key code]After carrying out exclusive logical addition of the one arbitrary partial bit string chosen from this partial bit string to each of other partial bit stringrespectivelycombine it and the first bit string is generatedCarry out exclusive logical addition of the second bit string of the same number of bits as said information key code to said first bit stringand the third bit string is generatedAfter dividing into two or more partial bit strings of the numbers of bits [bit string / said / third] and rotating only the predetermined number of bits on the right or the left within each of this partial bit stringAn information encryption method of one above-mentioned description or an information decoding method of two above-mentioned description which generating the fourth bit string unitedlydividing said fourth bit string into two or more partial bit stringschanging array order of each partial bit stringand generating.
[0013]4. Information encryption method of one above-mentioned description or information decoding method of two above-mentioned descriptionwherein said enciphering key code or said decryption key code is false random code sequence generated using value just because it did division of said work key code with said sector number.
[0014]5. In data encryption device which enciphers said digital information data when recording on information recording medium with sector number which divides digital information data into two or more sectorsand shows rank of sectorA code conversion means which carries out code conversion of the information key code peculiar to said digital informationand carries out raw [of the work key code]A data encryption device having an information encoding means which enciphers said digital information data which generated an enciphering key code from a work key code outputted from this code conversion meansand said sector numberand was sector-ized using this enciphering key code.
[0015]6. In information decoding device which decodes said digital information data of recording medium with which digital information data divided and

enciphered by two or more sectors is recorded with sector number which shows rank of sectorA key decoding means which decodes an information key code peculiar to said enciphered digital information which is supplied from other than said recording mediumA code conversion means which carries out code conversion of the information key code decoded in this key decoding meansand generates a work key codeA decryption key code is generated from a work key code generated in this code conversion meansand said sector number currently recorded on said recording mediumAn information decoding device having an information decoding means which decodes enciphered digital information which is acquired by reproducing said recording medium using this decryption key code.

[0016]7. Said code conversion means is divided into two or more partial bit string of the numbers of bits [information key code]The bit string division / adding means which combines it and generates the first bit string after carrying out exclusive logical addition of the one arbitrary partial bit string chosen from this partial bit string to each of other partial bit stringrespectivelyAn adding means which carries out exclusive logical addition of the second bit string of the same number of bits as said information key code to said first bit stringand generates the third bit stringA bit rotation means which generates the fourth bit string unitedly after dividing into two or more partial bit strings of the numbers of bits [bit string / said / third] and rotating only the predetermined number of bits on the right or the left within each of this partial bit stringdividing said fourth bit string into two or more partial bit stringsand changing array order of each partial bit string -- work key code **** -- a data encryption device of five above-mentioned description characterized by thingsor an information decoding device of six above-mentioned description.

[0017]8. Data encryption device of five above-mentioned description or information decoding device of six above-mentioned descriptionwherein said enciphering key code or said decryption key code is false random code sequence generated using value just because it did division of said work key code with said sector number.

[0018]9. Digital information data divided into two or more sectors is the information recording medium currently recorded with a sector number which shows rank of a sectorand said digital information dataAn information recording medium enciphering using an enciphering key code generated from a work key code which carried out code conversion of the information key code peculiar to said digital informationand said sector number.

[0019]

[Embodiment of the Invention]Before giving detailed explanation of the information encryption method of this inventionan information decoding methoda

data encryption devicean information decoding deviceand an information recording mediumthe outline of the information distribution system which is a field of the invention of this invention first is explained using drawing 1.
[0020]In the figurethe supplier of information has the following.
The information control means 1 which performs management of the information (contents) which is recorded on the recording medium 3and with which sale etc. are presentedgeneration management of an information key peculiar to informationetc.
A customer-relations-management means 5 to perform management of customer datageneration management of a distribution key or an authentication keyaccounting managementetc.

[0021]And in supplying predetermined information to a predetermined customer. Firstwhile it enciphers using the authentication key which approves acquisition of information to an information key and a customer peculiar to the informationand an information provider records the information for which a customer asks on the predetermined information recording medium 3 and supplies it to a customer in encryption / recording device 2It enciphers using a distribution key as information for generating the decode key used in order to decode the enciphered informationand by the card issuing means 6an information keyauthentication keys (or information corresponding to themetc.)etc. are recorded on the card 7and are distributed among a customer. A customer equips reproduction / decoding means 4 with the information recording medium 3 and the card 7 which were receivedand acquires predetermined information. An authentication key is the information peculiar to the group etc. to whom a customer or a customer belongs given beforehandand a distribution key is the information peculiar to the information reproduction/decoding device which a customer uses given beforehand.
[0022]In such an information distribution systemthis invention performs a new proposal about this encryption and decryption. That isthis invention divides digital information into two or more sectorsenciphers information for every sector using the encryption key generated based on the information key peculiar to the sector number and information which were given to each sectorand records the enciphered digital information data on a recording medium.
[0023]Heresince a sector number is a number peculiar to each sectoreach sector will be enciphered using an encryption key respectively peculiar to a sector. That isinformation is enciphered using the encryption key updated frequently (it is at intervals of about 0.003 second at working example explained in full detail below). Thussince an encryption key is updated at a short intervalit becomes very difficult to presume the encryption key used for it and its

decode key from the enciphered information.
[0024]An information key code is changed into another code in encryption and decryptionand the encryption key and the decode key are generated using the changed work key code. Even if two or more information keys which are mutually regular by this tend to be prepared and it is going to try presumption of a decode keysince regularity collapsespresumption of a decode key becomes difficult by this code conversion.
[0025]The case where DVD (Digital Versatile Disk) is used as a recording medium which records the enciphered information hereafter as one working example of the information encryption method of this inventionan information decoding methoda data encryption devicean information decoding deviceand an information recording medium is explained. As an information recording medium used by this inventionnot only DVD but other magnetic tapea magnetic disketc. are effective.
[0026]
[Example]Drawing 2 is a block diagram showing the example of composition of a ****** supply side with the enciphering device of this invention. the information (video information.) which presents sale etc. with the information control means 1 in the figure contents informationsuch as speech information and data informationand following contents information -- saying -- while holding as stockin order to manage itto encipher an information signal if needed and to record on a recording mediumencryption / recording device 2 is supplied. When supplying an information signal to encryption / recording device 2the information key code which is information peculiar to the contents information is supplied to encryption / recording device 2and the customer-relations-management means 5.
[0027]When the customer-relations-management means 5 manages a distribution keyan authentication keyetc. and supplies contents information to a customerit supplies an authentication key code to encryption / recording device 2. Using a distribution key codean information key code and an authentication key code are encipheredand it outputs to the card recording device 32records on the card shaped information recording medium (it is hereafter described as a card) 7and distributes among a customer (a useran information user). An authentication key is the peculiar information (for examplea membership number and a customer-relations-management number) for identifying the group etc. to whom a user or a user belongs.
A distribution key is the peculiar information (for exampleidentification numberssuch as a serial number of a device) for identifying the information reproduction / decoding means 4 which a user uses.

[0028]The information signal supplied to encryption / recording device 2 from

the information control means 1 is first inputted into MPEG coding / sector-ized means 8. MPEG coding / sector-ized means 8 performs compression encoding according the inputted information signal to an MPEG systemgenerates digital information dataand divides this digital information data into two or more sectors which comprise 2048 bytes further.
[0029]Thenin order to double with a DVD formatsector management informationa sector numberetc. are added to each sectorthe data sector which comprises 2064 bytes is builtand the encoding means 11a is supplied one by one.
[0030]The structure of the data sector built by this MPEG coding / sector-ized means 8 is shown in drawing 4. One data sector shown in drawing 4 (b) comprises EDC (4 bytes) which is error detection codes of IED (2 bytes)main data (2048 bytes)and main data which are error detection codes of ID information (4 bytes) and ID information. This ID information comprises sector information data (1 byte) and a sector number (3 bytes)as shown in drawing 4 (a). The sector-ized digital information data is stored by the above-mentioned main data area. A sector number shows the rank of each data sectorand is usually consecutive numbers from the first sector.
[0031]The information key code supplied to encryption / recording device 2 from the information control means 1 is inputted into the code converter 9a. The authentication key code supplied to encryption / recording device 2 from the customer-relations-management means 5 is also inputted into the code converter 9a. And the code converter 9a performs the predetermined operation and code conversion processing which are later mentioned between the information key code and authentication key code which were inputtedand supplies the work key code obtained as a result to the cryptographer stage 11a.
[0032]Herealthough the information key code is used as one of the encryption key generation elementsthe privacy of the encryption key and the decode key is improved by changing into another code the information key code supplied from the information control means 1. And the example of composition of the code converter 9a is shown in drawing 6and the procedure of the operation and code conversion processing is shown in drawing 7. In the procedure of lower **code conversion of the information key code is carried outand it is outputted as a work key code.
[0033]The information key code inputted is supplied to bit string division / adding machine 27. bit string division / adding machine 27 is arbitrary in the input code (information key code) supplied -- etc. -- it divides into two or more partial bit strings D0 which consist of bit lengthD1--D9 (drawing 7 (a)). And exclusive logical addition of the one partial bit string (although it is D4 in working exampleit does not restrict to this) is individually carried out to each remaining partial bit stringsand the new partial bit string (the first bit string) E0E1--E9 are obtained. Exclusive OR of D4 comrades is set to E4 =

D4 at this timewithout taking. And these partial bit strings E0E1--E9 are combineda new bit string is obtainedand it outputs to the adding machine 30 (drawing 7 (b)).

[0034]As opposed to the new bit string to which the adding machine 30 is supplied from bit string division / adding machine 27the authentication key code (drawing 7 (c).) of the numbers of bits [information key code / which are supplied from the customer-relations-management means 5] The bit string obtained by carrying out exclusive logical addition of the second bit string is divided into two or more partial bit strings (the third bit string) F0 of bit lengthsuch as arbitrationF1--F4and it outputs to the bit rotation machine 28 (drawing 7 (d)).

[0035]The bit rotation machines 28 are the partial bit string F0 suppliedF1--each partial bit string unit (inside of F0 and F1--) divided in F4It rotates on the right (drawing 7 (e))and only the predetermined number of bits obtains the partial bit string G0G1--G4 (the fourth bit string) (drawing 7 (f)). This partial bit string G0G1--G4 are supplied to the bit string transposition machine 29and change arbitrarily the partial bit string G0G1--the array order of G4. And it outputs to the information encoding means 11a by making into a work key code the bit string obtained as a result (drawing 7 (g)).

[0036]Since the code converter 9a explained above has the feature said that a work key code changes at random corresponding to it even if an input key code is changed into the work key code of a meaning and an input key code changes regularlyIt is very difficult to guess the decode key for decoding it from the information enciphered using such a work key code.

[0037]Although above-mentioned bit lengththe number of partitionsetc. of each partial bit string are arbitraryit is necessary to consider it as the same bit length as the code conversion means 9b used by the reproduction / decoding means 4 mentioned laterand the partial bit string of the number of partitions.

[0038]Based on the work key code supplied from the code converter 9athe information encoding means 11a enciphers the sector data supplied from MPEG coding / sector-ized means 8and supplies the enciphered sector data to ECC-code-izing / modulation means 12.

[0039]Herethe example of composition of the information encoding means 11a is shown in drawing 5and the operation is explainedreferring to drawing 4. In the figuresector data is inputted into the signal separator 22 and the sector decoder 23 as an input bit sequence. A work key code is inputted into the divider 21.

[0040]The sector decoder 23 carries out the detection decipherment of the ID information in sector dataand when an input bit sequence is during a main data area periodit supplies a division control signal (drawing 4 (d)) to the signal separator 22. A sector number is extracted and it outputs to the divider 21.

An initialization control signal (drawing 4 (c)) is supplied to M column code generator 24 at the start time (before becoming a main data area period) of each sector.
[0041]The signal separator 22 supplies the main data in sector data to the adding machine 26 according to the division control signal supplied from the sector decoder 23and it supplies the other data to the signal coupler 25.
[0042]On the other handthe divider 21 is supplied to the M sequence coder 24 by making a value into an initial value just because it did division of the work key code and obtained it as a result with the sector number supplied from the sector decoder 23. It generates a false random code sequence (enciphering key code) by making a value into an initial value just because it is supplied from the divider 21whenever an initialization control signal is supplied the M sequence coder 24 from the sector decoder 23and it outputs it to the adding machine 26.
[0043]By carrying out exclusion logical addition of the false random code supplied from the M sequence coder 24 to the main data supplied from the signal separator 22the adding machine 26 enciphers these and supplies the enciphered main data to the signal coupler 25. The signal coupler 25 outputs the sector data (drawing 4 (e)) which combined the ID informationIED data and copyright management information data which are supplied from the signal separator 22and the enciphered main data which are supplied from the adding machine 26and was enciphered.
[0044]Herethe sector number in ID information is a value peculiar to each sector like previous statement. Thereforethe M sequence coder 24 will generate a false random code sequence by making a value peculiar to the sector into an initial value for every sector. Thereforeeach sector is enciphered by a code string differentrespectively.
[0045]One sector is 2064-byte length like previous statement.
This is equivalent to a for [0.003 second] grade by real time reproduction. That isan enciphering pattern will change one after another at intervals of about 0.003 second. Thereforeeven if the enciphered data which was recorded on the information recording medium is reproducedthe data pattern is analyzed and it tries the decipherment of an encryption key/decode keyit is difficult to decode for such a short period of time.
[0046]Thusthe information encoding means 11a outputs the sector data row enciphered for every data sector to EC coding / modulator 12. And predetermined processing is performed to the enciphered sector data row which was outputted from the information encryption machine 11a by EC coding / [publicly known] modulator 12and the publicly known format means 13and it is recorded on the master disc 14. Based on this master disc 14the publicly known disk duplicate means 15 are usedthe disk 16 for playback is reproducedand a

user is supplied. When you do not need many disks 16 for playbackit may use the master disc 14 as an object for user supply.
[0047]By the key encoding means 31aan information provider enciphers an above-mentioned information key code and authentication key code using a distribution key coderespectivelysupplies the card recording device 32and records on the card 7. And the card 7 which recorded the information key code and authentication key code which did in this way and were enciphered by the distribution key code is distributed among a user. Neither a techniquenor the card recording device 32 and the card 7 of encryption need to be specificand can use various things. [encoding means / 31a / key]
[0048]Drawing 3 is a figure showing users' (information user side) example of composition. A user equips playback / decoding means 4 with the disk 16 for playback (information recording medium) with which the enciphered contents information was recordedand the card 7 with which information required in order to decode the enciphered information was recordedand does playback decoding of the enciphered contents information.
[0049]The publicly known information reproduction means 17 which the playback / decoding means 4 shown in the figure read data in the disk 16 for playbackand outputs digital dataPublicly known recovery / error correcting means 18 which an error correction is carried out using IED and EDC which are contained in a data sectorand restores to informationIt comprises the information decoding means 11bthe card decoding means 19the distribution key storing means 33the key decoding means 31band the code converter 9band the publicly known sector decomposition / MPEG decoding means 20. The code converter 9b and the information decoding means 11b are completely identical configurations with the code converter 9a and the information encoding means 11a in encryption / recording device 2 as stated aboverespectively.
It has the same operation and the same function.

[0050]The reproduction means 17 supplies the reproduction information acquired from the disk 16 for playback by playing to a recovery / error correcting means 18. A recovery / error correcting means 18 restores to reproduction informationcarries out error correction processingobtains the enciphered sector dataand supplies it to the information decoding means 11b.
[0051]On the other handthe card decoding means 19 reads the information key code and the enciphered authentication key code which are recorded on the card 7 and which were encipheredand supplies these to the key decoding means 31b.
[0052]The key decoding means 31b decodes the information key code and authentication key code which are enciphered using the distribution key stored in the distribution key storing means 33respectivelyand outputs an information key code and an authentication key code to the code converter 9b. The

distribution keys stored in the distribution key storing means 33 are the identification numbers (for exampleserial number etc.) of the device beforehand given to reproduction / decoding means 4.
The same thing as the distribution key stored in the customer-relations-management means 5 is used.
The card decoding means 19 and the key decoding means 31b can use various things and methods.
[0053]The example of composition of the code converter 9b is shown in drawing 6. Since this is the code converter 9a and identical configuration which were used by encryption / recording device 2 as stated abovedetailed explanation of the operation is omitted. And the information key code similarly supplied from the key decoding means 31b is changed into a work key code using the authentication key code supplied from the key decoding means 31band this is outputted to the information decoding means 11b.
[0054]The example of composition of the information decoding means 11b is shown in drawing 5. Although this is the information encoding means 11a as stated above and identical configuration and the detailed explanation is omittedthe false random code sequence outputted from the M sequence numerals generating means 24 is used as a decode key code. Thereforealthough the sector data which should be enciphered as an input bit sequence is inputted in the case of the information encoding means 11a and the sector data enciphered as an outputted bit sequence is outputtedIn the information decoding means 11bthe sector data enciphered as an input bit sequence is inputtedand the sector data which decoded the sector data enciphered as an outputted bit sequence is outputted. a work key code is with the case of encryptionand the case of decryption here -- the same Cord -- certain ** Thereforethe enciphered sector data is correctly decoded by the original sector data.
[0055]And the decoded sector is outputted to sector separation / MPEG decoding means 20and MPEG decoding is carried out and it is outputted to the original information signal.
[0056]
[Effect of the Invention]The information encryption methodthe information decoding methoddata encryption deviceand information decoding device information recording medium of this invention can perform powerful encryption by an easy means.
[0057]And since the information recording medium of this invention does not need to record the information about an encryption key/decode keyit is not necessary to secure the record section for itand is effective in the ability to use the record section of information efficiently.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a lineblock diagram showing an example of an information distribution system.

[Drawing 2]It is a lineblock diagram showing one working example of the data encryption device of this invention.

[Drawing 3]It is a lineblock diagram showing one working example of the information decoding device of this invention.

[Drawing 4]It is a figure showing the example of the sector structure of the information recorded on the information recording medium of this invention.

[Drawing 5]It is a lineblock diagram showing one working example of an information encoding means and an information decoding means.

[Drawing 6]It is a lineblock diagram showing one working example of a code converter.

[Drawing 7]It is a figure for explaining an example of operation by a code converter.

[Description of Notations]

1 Information control means
2 Encryption/recording device
3 Information recording medium
4 Reproduction/decoding means
5 Customer-relations-management means
6 Card issuing means
7 Card (card shaped information recording medium)
8 MPEG coding / sector-ized means
9a9b code converter (code conversion means)
11a Information encoding means
11b Information decoding means
12 ECC-code-izing / modulation means
13 Format means
14 Master disc
15 Disk duplicate means
16 The disk for playback
17 Information reproduction means
18 A recovery/error correcting means
19 Card decoding means
20 Sector separation / MPEG decoding means
21 Divider
22 Signal division means
23 Sector decoding means

24 M sequence coder
25 Signal coupling means
26 Adding machine
27 Bit string division / adding machine
28 Bit rotation means
29 Bit string transposition means
30 Adding machine
31a Key encoding means
31b Key decoding means
32 Card recording device
33 Distribution key storing means